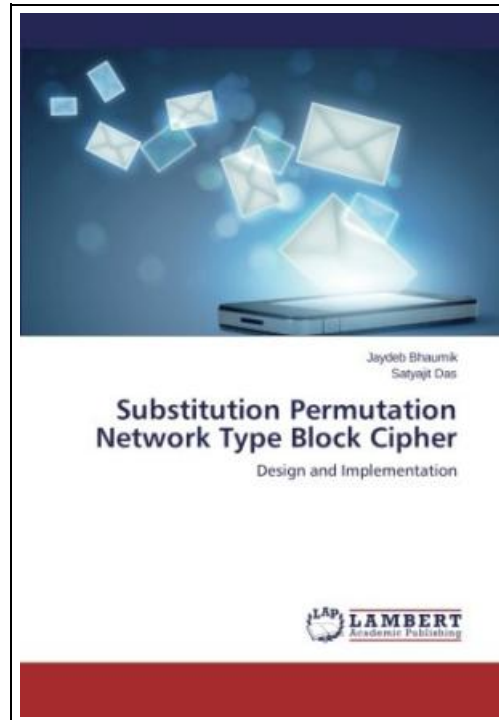


Substitution Permutation Network Type Block Cipher



Filesize: 2.03 MB

Reviews

The ebook is straightforward in read through preferable to comprehend. It is definitely simplified but shocks within the fifty percent of your pdf. Your lifestyle span is going to be transform when you total reading this publication.
(Dr. Jarrett Bednar)

SUBSTITUTION PERMUTATION NETWORK TYPE BLOCK CIPHER



Condition: New. Publisher/Verlag: LAP Lambert Academic Publishing | Design and Implementation | Cryptography is an important tool for achieving information security. It has found applications in smart card, mobile phones, sensor network and RFID. Information security mainly covers confidentiality, authentication, data integrity and non-repudiation. Block cipher is an important symmetric-key cryptographic primitive which is employed to provide confidentiality. Substitution permutation network (SPN)-type block cipher is one of them. Advanced Encryption System (AES) is the most popular SPN-type block cipher and used in many wired and wireless devices. Mathematical security of cryptographic algorithms is no more sufficient in present day applications. It is very much essential to pay attention on implementation weakness of cryptographic algorithms against statistical attacks, power analysis attack, fault attack, cache attack etc. Among these attacks, fault attack is an efficient way to break the security of many cryptosystems. In this work, a fault based attack on MDS-AES has been proposed. Further, in this research fault attack resistant SPN-type architectures have been introduced. Successful attempts have been made in incorporating these architectures into a FPGA chip | Format: Paperback | Language/Sprache: english | 68 pp.



[Read Substitution Permutation Network Type Block Cipher Online](#)



[Download PDF Substitution Permutation Network Type Block Cipher](#)

Related PDFs



Memoirs of Robert Cary, Earl of Monmouth

BiblioLife. Paperback. Book Condition: New. This item is printed on demand. Paperback. 142 pages. Dimensions: 8.0in. x 5.0in. x 0.3in. The Author of the Memoirs. The Memoirs here presented to the reader may be said to...

[Save](#) [ePub](#)

»



Gypsy Breynton

Echo Library. Paperback. Book Condition: New. Paperback. 88 pages. Dimensions: 9.0in. x 6.0in. x 0.2in. Hon. Gypsy Breynton, Esq., M. A., D. D., LL. D., c., c. Gypsy Breynton, R, R...

[Save](#) [ePub](#)

»



Aeschylus

BiblioLife. Paperback. Book Condition: New. This item is printed on demand. Paperback. 260 pages. Dimensions: 8.0in. x 5.0in. x 0.6in. This Translation of Aeschylus, an entirely new one, is designed as an Appendix to my...

[Save](#) [ePub](#)

»



Crochet: Learn How to Make Money with Crochet and Create 10 Most Popular Crochet Patterns for Sale: (Learn to Read Crochet Patterns, Charts, and Graphs, Beginner s Crochet Guide with Pictures)

Createspace, United States, 2015. Paperback. Book Condition: New. 229 x 152 mm. Language: English . Brand New Book ***** Print on Demand *****. Getting Your FREE Bonus Download this book, read it to the end and...

[Save](#) [ePub](#)

»



Would It Kill You to Stop Doing That?

Book Condition: New. Publisher/Verlag: Little, Brown Book Group | A Modern Guide to Manners | A laugh-out-loud guide to modern manners by acclaimed humorist, author, and Vanity Fair columnist Henry Alford. | A few years...

[Save](#) [ePub](#)

»